REMARKS/ARGUMENTS

Claim Rejections

The Examiner rejected pending claims 1-24 under 35 U.S.C. §102(e) as being unpatentable over Ault (US 6,338,064). Applicants have amended independent claims 1, 9, 17, and traverse the claim rejections.

Amended Independent Claims 1, 9, 17

Independent claims 1, 9, and 17 provide a method, system, and article of manufacture for accessing a control system in a server from a client, wherein the control system includes a logon program to enable the client to use a terminal emulation program to logon to the server to access a client process executing in the server to perform control system operations, further comprising:

requesting, with the client, a security context for the client including authorization to allow the client to access control system functions in the server, wherein the security context is associated with a client credential information including access for which the client is authorized;

impersonating the client, by the server, to generate the security context;

returning, with the server, the generated security context to the client;

transmitting, with a client program executing in the client, a control system command and the security context to access the control system in the server; and

based on the control system command, reconfiguring a printer object, wherein the requesting, the impersonating, the returning, the transmitting, and the reconfiguring are performed without using the logon program to enable the client to logon to the server.

Apart from correcting antecedent basis errors, Applicant has amended claims 1, 9, and 17 and the amended claims 1, 9, 17 include the following limitations:

(a) impersonating the client, by the server, to generate the security context, and returning the generated security context to the client.

(b) based on the control system command, reconfiguring a printer object, wherein the requesting, the impersonating, the returning, the transmitting, and the reconfiguring are performed without using the logon program to enable the client to logon to the server.

Support for the added limitations may be found in at least page 4: lines 4-9; page 6: lines 19-23; page 7: lines 9-10; and pages 4-12 of the specification.

The Examiner has rejected the independent claims 1, 9, and 17 under 35 U.S.C. §102(e) as being unpatentable over Ault (Office Action Page 2). The cited Ault (col. 6: lines 10-41; col. 6: lines 50-67; col. 7: lines 1-11; col. 7: lines 12-28) discusses accepting a client request at a server. The client request contains an authorization information that is analyzed by the server via a plug-in in the server. The server determines if the client can retrieve a document and if the client can retrieve the document then the server sends the document to the client.

The claims require requesting with the client a security context for the client, wherein the security context is associated with a client credential information including access for which the client is authorized, and wherein the server is impersonates the client to generate the security context. The server returns the generated security context to client. The client sends a control system command and the security context to the server. Based on the control system command, at least one printer object is reconfigured. Additionally, the requesting, the impersonating, the returning, the transmitting, and the reconfiguring are performed without using the logon program to enable the client to logon to the server.

Applicants request the Examiner note that the claim limitations require the security context to be associated with a client credential information including access for which the client is authorized and require the server to generate the security context by impersonating the client. The claims also require the server to return the generated security context to the client.

Nowhere does the cited Ault teach or disclose the claim limitation that the server returns the generated security context to the client. The Examiner cites col. 6, lines 58-67 of the cited Ault as discussing the claim requirement of returning with the server the generated security context to the client. Col. 6, lines 58-67 of the cited Ault is as follows: "The routine then

continues at step 90 with the session manager process 62 adding a "key" to the Windows NT registry of the Windows NT operating system on the server platform. The key is the "name" or other "identifier" (e.g., SID, which is a Windows NT Security Identifier that uniquely identifies the NT user) of the selected temporary Windows NT user. At step 92, the routine associates a "value" (e.g., a string) representing the path specification to the DCE credential file returned to the session manager 62 at step 88. Thus, these steps make the DCE credential." Therefore, the cited Ault discusses a credential file that is returned to the session manager (Ault: reference numeral 62). Applicants maintain that the session manager (Ault: reference numeral 62) is associated with the server and not with the client. For example, in FIG. 3 of the cited Ault, the client is referred to with the reference numeral 41, and the server (Ault: reference numeral 45) is associated with the session manager (Ault: reference numeral 62). Additionally, in Col. 5, lines 50-54, the cited Ault is as follows: "The system also includes a session manager control process 60 and a session manager process 62, each of which preferably are created by the server plug-in component 49 when the Web server 45 initializes." Therefore, the cited Ault discusses that the session manager process 62 is associated with the server, and created by the server plug-in component 49 integrated with the server (Ault: Col. 5: lines 37-41). Therefore, the cited Ault discusses that the credential is returned to the session manager process associated with the server, whereas the claims require returning the generated security context to the client.

Additionally, nowhere does the cited Ault teach or disclose the claim limitation of transmitting with a client program executing in the client, a control system command and the security context to access the control system in the server, wherein based on the control system command printer object is reconfigured. The Examiner cites col. 7, lines 1-11 of the cited Ault as discussing the claim requirement of transmitting with a client program executing in the client, a control system command and the security context to access the control system in the server. Col. 7: lines 1-11 of the cited Ault as follows: "accessible to the DCE cell (and, DFS, in particular) and thus, generally, associates the credential with the selected temporary NT user identity. As illustrated in FIG. 6, the Windows NT registry 63 (or some other desired storage

location) thus contains an entry 65 (comprising a name/identifier and value pair) that associates the selected NT user with a DCE credentials file. At step 94, the routine returns to the server plug-in 49 the name/identifier of the selected temporary NT user, together with the NT user's password. At step 96, control is then returned back to the server plug-in component 49." The routine that is returning to the server plug-in 49 the credential file in the cited Ault, (in step 94) is a server thread (Ault: col. 6: lines 10-14; lines 24-25). Therefore, the cited Ault discusses returning from within the server the credential file to the server plug-in integrated with the server, whereas the claims require transmitting from the client the control system command and the security context to access the control system in the server. Additionally, the steps discussed in the cited Ault are implemented in the server and associated with the server (Ault: Summary, Col 2: lines 60-61: "The invention preferably in implemented in a plug-in or other application executed by the Web server")

Additionally, nowhere does the cited Ault teach or disclose the newly added claim requirements that based on the control system command, reconfiguring at least one printer object, wherein the requesting, the impersonating, the returning, the transmitting, and the reconfiguring are performed without using the logon program to enable the client to logon to the server. In fact, the cited Ault teaches away from the claim requirements, because the cited Ault require logons from the client to the server. For example, in the cited Ault, when a browser user attempts to access a DFS file from a Windows NT system running the Web server and the server plug-in, the plug-in component prompts the browser user for a DCE user id and password (Ault: Summary: Ault: Col. 3: lines 2-5).

Additional reasons for the patentability of claims 1, 9, and 17 are given below:

The cited Ault discusses that the client requests a document from the server, whereas the claims require that the client requests a security context. The document is a protected file in Ault (Ault: col. 1 lines 10-12), where Ault further describes that the server supports files in the form of hypertext documents and objects (Ault, col. 4: lines 9-10). Nowhere does the cited Ault teach or disclose the claim requirement that the client requests a security context, wherein the security

context is associated with a client credential information including access for which the client is authorized, and wherein the server is capable of impersonating the client to generate the security context. The cited Ault discusses that the document that is requested by the Web browser (Ault: reference numeral 16) in the client (Ault: reference numeral 10) is a Web document, whereas the claims require the client to request a security context.

While the cited Ault does discuss impersonation of a client, the impersonation of the cited Ault is for obtaining a protected file for the client. The protected file discussed in Ault are Web documents (Ault: col 1: lines 9-12). The impersonation of the client discussed in Ault is for returning Web documents requested by the client, but the cited Ault does not teach or discuss the claim requirement of returning, with the server, the generated security context to the client. Therefore, not only is the Web document discussed in the cited Ault is different from the security context required by the claims, but the claim requirement of the server being capable of impersonating the client to generate the security context is neither taught nor disclosed by the cited Ault.

In the cited Ault, the client requests a Web document and the server impersonates the client to secure the Web document and return the Web document to the client. Even if for the sake of argument the Web document discussed in the cited Ault is interpreted to be the security context of the claim requirements (which the applicant disputes), nowhere does the cited Ault teach or disclose the claim requirement of transmitting with a client program executing in the client, the security context to access to the control system in the server. In contrast, the cited Ault discusses requesting the Web document from the client and receiving the Web document at the client.

Furthermore, nowhere does the cited Ault teach or disclose the claim requirement of the client requesting a security context, wherein the security context is associated with a client credential information including access for which the client is authorized, and wherein the server is capable of impersonating the client to generate the security context. Lines 53-65 of the cited Ault discusses a plug-in that facilitates users authentication so that uses of client machines may

use browsers to access documents. However, Ault discusses that the plug-in is at the server (Ault: page 5: lines 37-42) and the plug-in is used for authentication. The user authentication discussed in the cited Ault is for returning a document and does not teach or disclose the claim requirement of returning, with the server, the requested security context to the client.

Therefore nowhere does the cited Ault teach or disclose the claim limitation of requesting, with the client, a security context for the client including authorization to allow the client to access control system functions in the server, wherein the security context is associated with a client credential information including access for which the client is authorized; impersonating the client, by the server, to generate the security context; returning, with the server, the generated security context to the client; transmitting, with a client program executing in the client, a control system command and the security context to access the control system in the server; and based on the control system command, reconfiguring a printer object, wherein the requesting, the impersonating, the returning, the transmitting, and the reconfiguring are performed without using the logon program to enable the client to logon to the server.

Further, the claims require that the control system includes a logon program to enable the client computer to use a terminal emulation program to logon to the server to access a client process executing in the server to perform control system operations. Nowhere does the cited Ault discuss the claim requirement that the control system includes a logon program to enable the client computer to use a terminal emulation program to logon to the server to access a client process executing in the server to perform control system operations. Additionally, nowhere does the cited Ault teach or disclose the claim requirement that the requesting, the impersonating, the returning, the transmitting, and the reconfiguring are performed without using the logon program to enable the client to logon to the server.

For the above reasons, claims 1, 9, and 17 are patentable over the cited Ault, because the cited Ault does not teach or disclose all the claim limitations.

Claims 2-8, 10-16, 18-24

The Examiner has also rejected pending claims 2-8, 10-16, 18-24 that depend on the pending independent claims 1, 9, and 17 respectively. Applicants submit that these claims are patentable over the cited art because they depend from claims 1, 9, 17 respectively which are patentable over the cited art for the reason discussed above, and because the combination of the limitations in the dependent claims 2-8, 10-16, 18-24 and the base and intervening claims from which they depend provide further grounds of distinction over the cited art

Claims 2, 10, 18

Claims 2, 10, and 18 depend from claims 1, 9 and 17 respectively and further require that requesting the security client comprises the client requesting the server to impersonate the client to obtain the security context, further comprising accessing, with the server impersonating the client, the security context to return to the client.

The claims require that the client requests the server to obtain the security context by impersonating the client and returning the security context to the client.

Col. 6: lines 10-14 of the cited Ault discusses impersonating an NT user on a server thread attempting to access the protected resource. Coll 7: lines 12-28 of the cited Ault discusses returning a context handle. The context handle is for the server and server associated programs. Nowhere does the cited Ault disclose the claim requirement that the server impersonates the client for returning the security context to the client. If the Examiner maintains the rejection, the Examiner is requested to indicate where in the cited Ault (col. 6: lines 10-14; col. 7: lines 12-28) is the security context returned to the client.

For the above reasons, claims 2, 10, and 18 are patentable over the cited Ault, because the cited Ault does not disclose all the claim limitations.

Claims 3, 11, and 19

Claims 3, 11, and 19 depend from claims 2, 10, and 18 respectively and further require that the Distributed Computing Environment (DCE) protocol is used to provide the client security context, wherein the client uses the sec_login_become_initiator DCE command to request the server to impersonate the client, wherein the server uses the sec_login_become_impersonator DCE command to impersonate the client to obtain the security context.

The claims require the client to use the sec_login_become_intiator DCE command to request the server to impersonate the client, wherein the server uses the sec_login_become_impersonator DCE command to impersonate the client to obtain the security context.

The cited Ault (col. 7, lines 54-58, 60-67; col. 8, lines 1-19) discusses how the server impersonates the client within the DCE protocol and further discusses login commands. Nowhere does the cited Ault disclose the claim requirement of the client using the sec_login_become_intiator DCE command to request the server to impersonate the client, wherein the server uses the sec_login_become_impersonator DCE command to impersonate the client to obtain the security context. In fact, there is no mention at all of any sec_login_become_intiator DCE command or sec_login_become_impersonator DCE command in the cited Ault.

For the above reasons, claims 3, 11, and 19 are patentable over the cited Ault, because the cited Ault does not disclose all the claim limitations.

Claims 4, 12, and 20

Claims 4, 12, and 20 depend from claims 1, 9 and 17 respectively and further require converting, with the server, the security context transmitted through the client program to a pointer to credential information of the client;

determining from the credential information, with the server, whether the client is authorized to invoke the transmitted control system command; and

executing, with the server, the control system command transmitted by the client if the client is authorized to invoke the command.

The Examiner Col. 7: lines 30-36 of the cited Ault discusses processing at the server a protected resource requested by the user. Applicants maintain that the protected resource requested by the user is different from the claim requirement of the security context transmitted through the client program. The protected resource discusses in the cited Ault may possibly be a protected file that is not accessible without permission to the client.

The claims require converting the security context transmitted through the client program to a pointer to a credential information of the client. The cited Ault discusses whether the user identity of a thread corresponding to the client has any associated credential. If so, access is granted to the client. Nowhere does the cited Ault disclose the claim requirement of converting the security context transmitted through the client program to a pointer to a credential information of the client.

For the above reasons, claims 4, 12, and 20 are patentable over the cited Ault, because the cited Ault does not disclose all the claim limitations.

Claims 5, 15, 21

Claims 5, 15, 21 depends on claims 1, 9, 17 respectively and require that the client computer includes a different operating system than the server, wherein the client program executing in the client interacts with the client process executing in the server to perform control system operations.

The cited Ault (col. 4, lines 2-9, 18-22) discusses browsers on a client, and a server having an operating system. Nowhere does the cited Ault teach or disclose that the client and the server must have different operating systems as required by the claims, in combination with the

claim requirement that the client program executing in the client interacts with the client process executing in the server to perform control system operations.

For the above reasons, claims 5, 15, and 21 are patentable over the cited Ault, because the cited Ault does not disclose all the claim limitations.

Claims 6, 14, and 22

Claims 6, 14, and 22 depend from claims 1, 9 and 17 respectively and further require that the client requests the security context through a remote procedure call.

The cited Ault discusses a Web server component running on the server that provides various security and other function and also discusses how the server plug-in component on the server calls the session manager through a remote procedure call. Nowhere does the cited Ault disclose the claim requirement that the client requests the security context through a remote procedure call. The remote procedure call (col. 6: lines 42-44) discussed in the cited Ault is for the server plug-in component to call the session manager (Ault: reference numeral 62). The cited Ault teaches away from the claims because in the cited Ault the remote procedure call is from the server to the session manager associated with the server, whereas the claims require making a remote procedure call from the client. Col. 5: lines 35-37 of the cited Ault cited by the Examiner do not discuss remote procedure calls.

For the above reasons, claims 6, 14, and 22 are patentable over the cited Ault, because the cited Ault does not disclose all the claim limitations.

Claims 7, 15, 23

Claims 7, 15, and 23 depend from claims 1, 9, and 17 respectively and further require that the control system is a printing systems manager to control printers and printer related objects managed by the server.

The Examiner cites Col. 1, lines 40-45 and col. 5, lines 14-18 of the cited Ault as discussing the claim requirements. Col. 1, lines 40-45 discusses that distributed file services may

be used in printing services. Col. 5, lines 14-18 of the cited Ault discusses data sharing for authentication. Nowhere does the cited Ault teach or disclose the claim requirement that control system is a printing systems manager to control printer and printer related objected managed by the server.

For the above reasons, claims 6, 14, and 22 are patentable over the cited Ault, because the cited Ault does not disclose all the claim limitations.

Claims 8, 16, and 24

Claims 8, 16, and 24 depend from claims 7, 15, and 23 respectively and further require that the printer system manager command transmitted by the client comprises a command to reconfigure at least one printer object, thereby allowing the client computer to perform administrative functions.

The cited Ault (col. 7, lines 44-49) discusses that the server returns the request file to the client to complete servicing of the original requests. A routine then continues with the server returning the user identity back to the session manager pool and the server making a remote procedure call to release the user. Nowhere does the cited Ault disclose the claim requirement that the printer system manager command transmitted by the client comprises a command to reconfigure at least one printer object, thereby allowing the client computer to perform administrative functions.

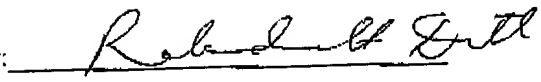
For the above reasons, claims 8, 16, and 24 are patentable over the cited Ault, because the cited Ault does not disclose all the claim limitations.

Conclusion

For all the above reasons, Applicant submits that the pending claims 1-24 are patentable over the art of record. Should any additional fees, beyond those indicated, be required, please charge Deposit Account No. 50-0585.

The attorney of record invites the Examiner to contact him at (310) 553-7977 if the Examiner believes such contact would advance the prosecution of the case.

Dated: June 7, 2004

By: 

Rabindranath Dutta

Registration No. 51,010

Please direct all correspondences to:

Rabindranath Dutta

Konrad Raynes Victor & Mann, LLP

315 South Beverly Drive, Ste. 210

Beverly Hills, CA 90212

Tel: 310-557-2292

Fax: 310-556-7984